

<b>Notice of Allowability</b>	Application No.	Applicant(s)
	09/668,426	MEDVINSKY, ALEXANDER
	Examiner Aravind K Moorthy	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to 10/21/04.
2.  The allowed claim(s) is/are 13.
3.  The drawings filed on 9/22/00 are accepted by the Examiner.
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All
  - b)  Some\*
  - c)  None
 of the:
  1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
  - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of
 Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1.  Notice of References Cited (PTO-892)
2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
3.  Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4.  Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5.  Notice of Informal Patent Application (PTO-152)
6.  Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_.
7.  Examiner's Amendment/Comment
8.  Examiner's Statement of Reasons for Allowance
9.  Other \_\_\_\_\_.

  
AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

**DETAILED ACTION**

1. Claim 13 is pending in the application.
2. Claims 1-18 and 14-21 have been cancelled.
3. Claim 13 has been allowed.

**EXAMINER'S AMENDMENT**

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Vobach on 11/3/04.

The application has been amended as follows:

Claim 13 (amended) A method of conveying a key from a server to a client comprising:  
generating a wakeup message at said server;  
generating a server nonce at said server;  
conveying said wakeup message and said nonce to said client;  
generating an AP request message at said client;  
conveying a client nonce and said AP request message to said server;  
confirming that said client nonce conveyed with said AP request message  
matches said server nonce generated at said server.

***Allowable Subject Matter***

4. Claim 13 is allowed.

The following is an examiner's statement of reasons for allowance.

As to independent claim 13, prior art teaches generating a wakeup message at the server. Prior art teaches generating a server nonce at the server. Prior art teaches conveying the wakeup message and the nonce to the client. Prior art teaches generating an AP request message at the client. Prior art teaches conveying a client nonce and the AP request message to the server. All the above taught by Liao et al U.S. Patent No. 6,148,405.

However, prior art does not disclose, teach or fairly suggest confirming that the client nonce conveyed with the AP request message matches the server nonce generated at the server.

The closest prior art to the current application was Liao et al U.S. Patent No. 6,148,405. The current application differs from Liao et al U.S. Patent No. 6,148,405 in that the server is satisfied with the fact that the client is known, namely Encry [C-nonce, C-nonceModified] in the received SR are successfully decrypted with the shared secret encrypt key, the step one in the client authentication is successful and a corresponding session key is generated and stored with the server proto session entry. Liao et al U.S. Patent No. 6,148,405 also differs from the current application in that the S-nonce generated by the server is generally different from the C-nonce generated by the client. Therefore, it would have not made sense to modify Liao et al U.S. Patent No. 6,148,405 so that the client would have been verified by the nonce conveyed with the AP request message because they would possibly have been different nonces.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy  
November 3, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100